MOTOROLA SOLUTIONS

DIMETRA™

DIMETRA X Core

Standalone Authentication Centre (AuC) Server Restoration

Backup and Restore

System Release 9.1.1

MAY 2025

MN006784A01-B

Intellectual Property and Regulatory Notices

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

License Rights

The purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end-users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU and UK countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

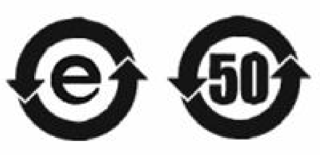
Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

CMM Labeling and Disclosure Table

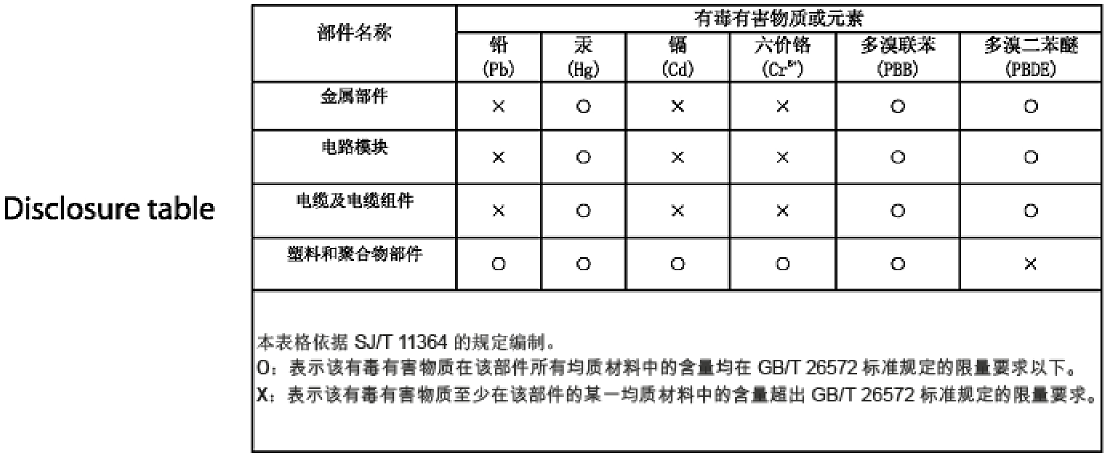
The People's Republic of China requires that our products comply with China Management Methods (CMM) environmental regulations. (China Management Methods refers to the Regulation Management Methods for Controlling Pollution by Electronic Information Products.) Two items are used to demonstrate compliance; the Label and the Disclosure Table.

The label is placed in a customer visible position on the product. The first of the following examples means that the product contains no hazardous substances; the second means that the product contains hazardous substances, and has an Environmental Friendly Use Period (EFUP) of fifty years.



The Environmental Friendly Use Period (EFUP) is the period (in years) during which the Toxic and Hazardous Substances contained in the Electronic Information Product (EIP) will not leak or mutate causing environmental pollution, or bodily injury from the use of the EIP.

The Disclosure Table, printed in simplified Chinese, is included with each customer order. An example of a Disclosure Table (in Chinese) follows:



Disclosure table

部件名称	有毒有害物质或元素					
	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr^{6+})	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
金属部件	×	○	×	×	○	○
电路模块	×	○	×	×	○	○
电缆及电缆组件	×	○	×	×	○	○
塑料和聚合物部件	○	○	○	○	○	×

本表格依据 SJ/T 11364 的规定编制。
O：表示该有毒有害物质在该部件所有均质材料中的含量均在 GB/T 26572 标准规定的限量要求以下。
X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 标准规定的限量要求。

Service Information

Technical & Repair Support (for Contracted Customers Only)

If you would like to contact the Motorola Solutions Customer Care team, use the appropriate contact details below. Please be prepared to provide your contract number, product serial numbers, and detailed issue description for a faster response and a resolution. If the support request is Technical Support related, the request will be handled by the Technical Support Operations (TSO) team. This team of highly skilled professionals provides Technical Support to help resolve technical issues and quickly restore networks and systems. If you are unsure whether your current service agreement entitles you to benefit from this service, or if you would like more information about the Technical or Repair Support Services, contact your local customer support or account manager for further information.

Contact Details

Technical Requests: techsupport.emea@motorolasolutions.com

Repair Support: repair.emea@motorolasolutions.com

Contact Us: https://www.motorolasolutions.com/en_xu/support.html

Parts Identification and Ordering

If you need help in identifying non-referenced spare parts, direct a request to the Customer Care Organization of a local area Motorola Solutions representative. Orders for replacement parts, kits, and assemblies should be placed directly at the local distribution organization of Motorola Solutions or through the Extranet site Motorola Online at https://emeaonline.motorolasolutions.com.

Document History

Version	Description	Date
MN006784A01-A	Initial version of the *Standalone Authentication Centre (AuC) Server Restoration* manual.	June 2020
MN006784A01-B	Updated section: ● Installing the External Modem Driver for KVL to AuC/PrC Communication on page 32	May 2025

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About Standalone Authentication Centre (AuC) Server Restoration

This manual describes how to perform restoration of the Standalone AuC Server, including hardware, software and data restoration of all application servers.

What Is Covered in This Manual?

This manual contains the following chapters:

- Server Software Restoration on page 18
- Primary/Secondary AuC Standalone Server Application Restoration on page 35

Related Information

Document Title	Description
Glossary	The glossary provides definitions of terms, abbreviations, and acronyms used in the DIMETRA system documentation.
Documentation Overview	This document provides a list of all documents delivered with your DIMETRA system.
System Overview	This manual explains basic radio system concepts, call processing basics, and an introduction to the various components and processes associated with the DIMETRA system. The manual provides the background needed to comprehend DIMETRA system theory of operation. It also provides functional descriptions of equipment and subsystems, and describes the role of the numerous network management software applications used in the system.
Enhanced Software Update User Guide	This manual describes the Enhanced Software Update feature, which provides backup and restore functionality, and upgrade functionality.
Authentication Centre (AuC) User Manual	This manual contains the configuration and operation procedures for the Authentication Centre (AuC). It contains reference information and detailed descriptions of the GUI.
Clear Authentication Centre (AuC) User Manual	This manual contains the configuration and operation procedures for the Clear Authentication Centre (CAuC). It contains reference information and detailed descriptions of the GUI.
Authentication and Encryption Overview	This manual gives an overview of the authentication and air interface encryption features in the DIMETRA system. It includes: ● Description of the authentication and air interface encryption features ● Description of the different aspects of secure encryption key management ● Procedures for configuring these features in your system
CryptR Instruction Manual	This manual covers hardware installation, main end-user operations and a proper maintenance of a range of devices based on the CryptR hardware platform.

Table continued…

Document Title	Description
Network Security	This manual describes all necessary actions to install, configure and maintain the network security feature within the DIMETRA system. The intention of the manual is to enable the reader to deploy the best possible level of security, which will protect the system against viruses, unauthorized authentication or attacks of hackers. The network security feature provides virus protection, authentication, and firewall protection.
Network Management Servers	This manual describes the Network Management (NM) Servers used in the DIMETRA system. The NM servers are comprised of User Configuration Server (UCS), System Statistics Server (SSS), Zone Database Server (ZDS), Air Traffic Router Server (ATR), Zone Statistics Server (ZSS) and Unified Event Manager (UEM) Server. Detailed procedures for installation, configuration and operation are included.
Network Management Client	This manual provides an introduction to the hardware and software components associated with the Network Management (NM) Client. Detailed procedures for installation, configuration and operation are included.
HP ProLiant Gen9 Server Platform Restoration	This manual describes how to restore a Gen9 server platform in case of a failure.
Common Server and Client Platform Restoration	This manual describes how to restore a Gen10 server platform in case of a failure. It contains information on replacing the hardware, as well as RAID/BIOS/iLO configuration.

Icon Conventions

The documentation set is designed to give the reader more visual clues. The following graphic icons are used throughout the documentation set.

⚠ DANGER: The signal word DANGER with the associated safety icon implies information that, if disregarded, will result in death or serious injury.

⚠ WARNING: The signal word WARNING with the associated safety icon implies information that, if disregarded, could result in death or serious injury, or serious product damage.

⚠ CAUTION: The signal word CAUTION with the associated safety icon implies information that, if disregarded, may result in minor or moderate injury, or serious product damage.

CAUTION: The signal word CAUTION may be used without the safety icon to state potential damage or injury that is not related to the product.

IMPORTANT: IMPORTANT statements contain information that is crucial to the discussion at hand, but is not CAUTION or WARNING. There is no warning level associated with the IMPORTANT statement.

NOTE: NOTICE contains information more important than the surrounding text, such as exceptions or preconditions. They also refer the reader elsewhere for additional information, remind the reader how to complete an action (when it is not part of the current procedure, for instance), or tell the reader where something is on the screen. There is no warning level associated with a notice.

Style Conventions

The following style conventions are used:

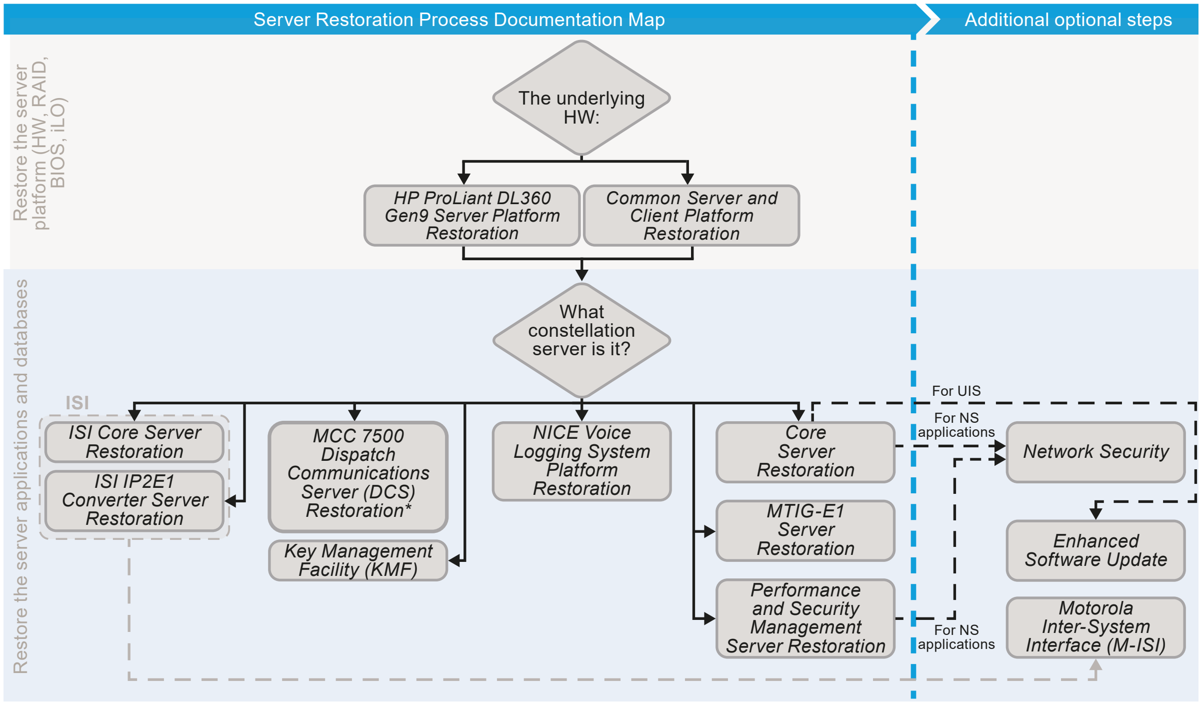
Convention	Description
Bold	This typeface is used for names of, for instance, windows, buttons, and labels when these names appear on the screen (example: the **Alarms Browser** window). When it is clear that we are referring to, for instance, a button, the name is used alone (example: Click **OK**).
`Monospacing font`	This typeface is used for words to be typed in exactly as they are shown in the text (example: In the **Username** field, enter: `Admin`).
	This typeface is used for messages, prompts, and other text displayed on the computer screen (example: `A new trap destination has been added`).
`<Monospacing font in bold Italic>`	This typeface is used with angle brackets as placeholders for a specific member of the group that the words represent (example: ***`<router number>`***). **NOTE:** In sequences to be typed in, the angle brackets are omitted to avoid confusion whether to include the angle brackets in the text to be typed.
CAPITAL LETTERS	This typeface is used for keyboard keys (example: Press Y and press ENTER).
Italic	This typeface is used for citations. A citation usually is the name of a document or a phrase from another document (example: *DIMETRA System Overview*).
→	An → (arrow pointing right) is used for indicating the menu or tab structure in instructions on how to select a certain menu item (example: **File** → **Save**) or a certain sub-tab.

Chapter 1

Server Software Restoration

Figure 1: Server Restoration Process Documentation Map

This figure presents the relation between manuals describing how to restore a server in a DIMETRA system.


Server Restoration Process Documentation Map
Additional optional steps
Restore the server platform (HW, RAID, BIOS, iLO)
The underlying HW:
HP ProLiant DL360 Gen9 Server Platform Restoration
Common Server and Client Platform Restoration
Restore the server applications and databases
What constellation server is it?
ISI
ISI Core Server Restoration
ISI IP2E1 Converter Server Restoration
MCC 7500 Dispatch Communications Server (DCS) Restoration*
Key Management Facility (KMF)
NICE Voice Logging System Platform Restoration
Core Server Restoration
MTIG-E1 Server Restoration
Performance and Security Management Server Restoration
For UIS
For NS applications
For NS applications
Network Security
Enhanced Software Update
Motorola Inter-System Interface (M-ISI)

Before you begin any restoration activities, ensure the server platform is configured properly. For details on the technical specification and hardware setup, see the *Common Server and Client Platform Restoration* manual or the *HP ProLiant DL360 Gen9 Server Platform Restoration* manual.

1.1 Server Restoration Prerequisites

Before restoring a server, ensure that you have the required software, passwords, licenses, and other necessary items listed in the table below.

IMPORTANT: Before starting the restoration procedures, check for any new Motorola Solutions Technical Notifications (MTNs).

Table 1: Standalone Authentication Centre Server Restoration Prerequisites

Type	Description
Software	*AIE-TEA1/AIE-TEA2/AIE-TEA3*
	System Accounts and Keys
	Core Software without AIE without SSL
	Flexible IP Plan (if required)

Table continued…

Type	Description
	ESET AntiVirus License (if required; not used during the server installation stage)
	Motopatch for Linux (optional)
	Motopatch for Windows (optional)
Other	Password list
	iLO license
	iLO interface IP address
	iLO credentials: user name and password
	System Accounts ID
	System Keys ID

NOTE: When installing or reinstalling the application server from the USB images, use a bundle of USB media appropriate for the used version of the USB image. Do not mix USB media from different bundles, unless you are informed to do so.

1.2 Restoring the Primary/Secondary Standalone AuC Server Application

Prerequisites: Connect the network interface card of the server.

IMPORTANT:

On HP DL360 Gen10 servers, you must use only the front horizontal USB 2.0 port located above the CD/DVD drive. If a serial adapter is inserted in this port, you must move it to another USB port or, if it is impossible, remove it. However, after the installation is complete, devices must be reconnected and rescanned by using iGAS. See "Rescanning the Devices by using iGAS" in the *Common Server and Client Platform Restoration*.

On HP DL360 Gen9, you can use any USB port, but you must first disable the USB 3.0 mode. See "Disabling USB 3.0 Support" in the *HP ProLiant DL360 Gen9 Server Platform Restoration* manual.

Procedure:

1. Connect directly to the server by using a KVM or a monitor and keyboard.
2. Perform one of the following actions:
   - If the server is off, insert the *Core Software without AIE without SSL* USB stick, and apply power to the server.
   - If the server is on, insert the *Core Software without AIE without SSL* USB stick, and reboot the server.

   IMPORTANT: If you are using the HPE Gen10 Server, do **not** use the iLO USB port.
3. On the **HP ProLiant** start-up screen, enter the **Boot Menu** by pressing F11.
4. From the list, select **USB**, and press ENTER.

   The server boots from the installation USB.

5. From the GRUB menu, select the entry starting with "DIPS".

   NOTE: The KVM Hypervisor boot may take a couple of minutes.

6. If the `Found gas.conf from previous installation. Would you like to use it and proceed with server installation? [Y/N]?` message appears, perform one of the following actions:

   - If you upgrade from D9.0.X/D9.1.0 to D9.1.1 and want to preserve the previous configuration of the server, enter: `Y`
   - In other cases, enter: `N`

   If you entered `Y`, the installation process starts. After approximately 20 minutes, the server reboots automatically. Skip to step 29.

7. At the `Do you want to continue the installation (y,n) [y]?` prompt, enter: `y`

8. At the prompt with the list of available cluster types, enter the number corresponding to the cluster type of your choice:

   ```
   1. DIMETRA Core Cluster 2. DIMETRA ISI Cluster Enter Cluster type (1-2):
   ```

9. Under the list of available constellations, enter the number corresponding to the server of your choice.

10. At the `Do you want to install with Customized IP Plan (y,n) [n]` prompt, perform one of the following actions:

If…	Then…
If you want to use the default IP plan,	enter: `n` and answer the following questions: a. `Enter the zone id (1-56)?` b. `Enter the cluster id (1-16)?`
If you want to use Customized IP Plan,	enter: `y` and answer the following questions: a. `Enter the zone id (1-56)?` b. `Enter the zone octet (1-127)?` c. `Enter the cluster id (1-16)?` d. `Enter the cluster octet (1-127)?`

    The following message appears:

    ```
    Enter the lowest zone octet number in the local cluster (1-127)? Enter the lowest
    zone octet number in the local MSO (1-127)?
    ```

11. Enter the lowest zone octet number in the local cluster and in the local MSO.

    The following message appears for the Primary Standalone AuC Server:

    ```
    Shall "Authentication Centre (auc_A)" be installed (y,n)[n]?
    ```

    The following message appears for the Secondary Standalone AuC Server:

    ```
    Shall "Authentication Centre (auc_B)" be installed (y,n)[n]?
    ```

12. Enter the applicable letter.

13. At the `Is Geographic & Local Redundancy system capable (y,n)?` prompt, enter the applicable letter.

    If you entered `n`, continue to step 15.

14. Select Geographic and Local Redundancy MSO localization by entering an applicable letter.

15. **If you entered** y **in step 12:** At the prompt, enter the number reflecting the AuC role in the system.

    The following message appears:

    ```
    Disable the PrC functionality on the Enhanced AuC (y,n) [n]?
    ```

16. Enter the applicable letter.

    The installer prompts you to enter the System Accounts ID.

17. Enter the System Accounts ID by using numerals and capital letters (five characters).
18. Enter the System Keys ID.

    The following message appears:

    ```
    Forward the System Logs (Syslogs) to Centralized Event Logging server? (y,n) [n]?
    ```

19. Enter the applicable letter.

    If you chose to forward logs to the Centralized Event Logging Server, the following messages appear:

    ```
    Please enter the primary syslog server address:
    ```

    ```
    Please enter the second syslog server address:
    ```

20. Enter the addresses of the syslog servers.

    The following message appears:

    ```
    Install AV Protection on All Application Servers? (y,n) [n]?
    ```

21. Enter the applicable letter.

    If you chose to install AV Protection, the following message appears:

    ```
    Enter the Zone ID for AV Server that manages AV Clients in this System (1-56):
    ```

22. Enter the appropriate value.

    The following message appears:

    ```
    Enter the Zone ID for AV Proxy that manages AV Clients in this Zone (1-56):
    ```

23. Enter the appropriate value.

    The following message appears:

    ```
    Do you have subscription for Security Update Service (y,n) [n]?
    ```

24. Enter: y or n

    The list of zones appears.

25. Enter the number for your zone.

    The list of time zones appears.

26. Enter the number for your time zone.

    A prompt with installation details and the following message appear:

    ```
    Confirm the configuration settings are correct (y,n) [y]?
    ```

27. If the installation settings are correct, enter: `y`

    NOTE: If you enter `n`, the installation process returns to the HPE menu.

    The following message appears:

    ```
    Do you want to proceed with the server installation (y,n) [y]?
    ```

28. Start the installation process by entering: `y`

    NOTE:

    If you enter `n`, the following message appears:

    ```
    !!!!!!!!!!!!!!!! WARNING !! WARNING !! WARNING !!!!!!!!!!!!!!!! Aborting the
    installation will not install the new software. Do you want to proceed with
    the server installation (y,n) [y]?
    ```

    The installation process starts and the server reboots automatically.

29. Follow on-screen instructions and, when prompted by the system, insert an appropriate installation USB stick.

    The full installation process may take up to several hours. The USB stick sequence depends on your system configuration and the options you selected in the initial part of the installation process.

    NOTE: Do **not** insert multiple USB sticks simultaneously. It is recommended to use a single USB port for installation. Remove the previous USB stick before you insert a new one.

30. At the `Do you have additional software on another installation USB media (y,n) [n]?` prompt, enter: `y`

31. Insert the appropriate AIE-TEA1/AIE-TEA2/AIE-TEA3 USB media, containing non-clear Authentication Centre software.

32. Select the AuC `.iso` file by entering the number and confirm if you want to load this file.

33. Exit the menu with additional software selection by entering: `q`

34. At the `Do you have additional software on another installation USB media (y,n) [n]?` prompt, if you do not want to install any additional software, enter: `n`

35. After the installation, change the **ilouser** and **Administrator** passwords. See Changing the iLO User Password on page 32.

Postrequisites: Remove all installation USB sticks from the server.

1.3 Logging On to the Server

Using an appropriate IP address and a PuTTY client, you can log on to a server or Improved Generic Application Server (iGAS) to re-install, configure, or restart a server.

Prerequisites: Power on the server.

Procedure:

1. Start PuTTY.
2. Optional: In the **PuTTY Configuration** window, in the **Category** navigation pane, expand the **SSH** node and select **Kex**.
3. Optional: In the **Options controlling SSH key exchange** pane, from the **Algorithm selection policy** list, select **Diffie-Hellman group 14** and click **Up**, until **Diffie-Hellman group 14** appears on the top of the list.
4. In the **Category** navigation pane, click **Session**.

5. In the **Basic options for your PuTTY session** pane, in the **Host Name (or IP address)** field, enter the IP address of the server. See your DIMETRA IP Plan.

   At the first attempt to log on, the **PuTTY Security Alert** window appears. For details on messages appearing when establishing the SSH session, see Messages Appearing when Establishing a Secure Session on page 23.

6. Start the session by clicking **Open**.
7. In the **PuTTY Security Alert** window, perform one of the actions:
   - To add the server rsa2 key to the PuTTY cache and connect, click **Yes**.
   - To connect without adding the server rsa2 key to the PuTTY cache, click **No**.
8. At the logon prompt, enter the user logon name.
9. At the password prompt, enter the current password.

1.3.1 Messages Appearing when Establishing a Secure Session

When establishing a secure session with iGAS or an application server, messages appear indicating different server states and possible risks.

Thie following table contains example messages likely to appear when logging on to a server.

NOTE: The IP addresses and RSA key fingerprints are unique per server and vary depending on the system configuration.

Table 2: Messages Appearing when Establishing a Secure Session

Message Example	Explanation
The authenticity of host '*<XXX.XX.XXX.X>* (*<XXX.XXX.XXX.XXX>*)' can't be established. RSA key fingerprint is *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>*. Are you sure you want to continue connecting (yes/no)? where *<XXX.XXXX.XXX.XXX>* is the IP address of the host and *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* are RSA key fingerprints of the server.	This message, or a similar message depending on the SSH client used, is normal and expected to appear at the first attempt to log on to a server.
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is. The server's rsa2 key fingerprint is: ssh-rsa *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting. If you want to carry on connecting just once, without adding the key to the cache, hit No. If you do not trust this host, hit Cancel to abandon the connection. where *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* are RSA key fingerprints of the server.	This message, or a similar message depending on the SSH client used, is normal and expected to appear at the first attempt to log on to a server.
@@ @@ @ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @	If the attempt to log on to a server occurs after the server re-

Table continued…

Message Example	Explanation
@@@ @@ IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY! Someone could be eavesdropping on you right now (man-in-the-middle attack)! It is also possible that a host key has just been changed. The fingerprint for the RSA key sent by the remote host is *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>*. Please contact your system administrator. Add correct host key in /root/.ssh/known_hosts to get rid of this message. Offending RSA key in /root/.ssh/known_hosts:42 RSA host key for *<XXX.XXX.XXX.XXX>* has changed and you have requested strict checking. Host key verification failed. where *<XXX.XXXX.XXX.XXX>* is the IP address of the host and *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* are RSA key fingerprints of the server.	storation, discard this or similar messages and proceed with the procedure. If the server did not undergo the process of restoration and this or a similar message appears during the normal use of the system, it is an indication of a potential security breach. ⚠ **WARNING:** Regardless of the possible cause for displaying the messages, notify the system administrator about a potential security breach.
WARNING - POTENTIAL SECURITY BREACH! The server's host key does not match the one PuTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server. The new rsa2 key fingerprint is: ssh-rsa *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* If you were expecting this change and trust the new key, hit Yes to update PuTTY's cache and continue connecting. If you want to carry on connecting but without updating the cache, hit No. If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice. where *<yyy:yyy:yyy:yyy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy:yy>* are RSA key fingerprints of the server.	If the attempt to log on to the server occurs after the server restoration, discard this or similar messages and proceed with the procedure. If the server did not undergo the process of restoration and this or a similar message appears during the normal use of the system, it is an indication of a potential security breach. ⚠ **WARNING:** Regardless of the possible cause for displaying the messages, notify the system administrator about a potential security breach.

1.4 Logging On to iGAS Through a KVM Switch

Before performing any operations in the iGAS menu of a server, connect directly to the server by using a Keyboard Video Mouse (KVM) switch or a monitor and a keyboard, and log on with one of the user accounts.

Prerequisites: Power on the server.

Procedure:

1. Connect directly to the server by using a KVM switch or a monitor and a keyboard.
2. At the logon prompt, enter the user logon.
3. At the password prompt, enter the password.

   The main menu for the selected user appears.

1.5
Checking the Installation Log

Accessing the installation log allows you to verify if it contains any unresolved errors.

Prerequisites: Log on to iGAS as **instadm** by performing one of the following actions:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon as **instadm**, verify that the **Installation Administrator Main Menu** appears.
2. Enter the number for **View Installation Log**.

   The installation log status message appears.
3. Press SPACE several times to continue to the end of the message.
4. View the status information to verify that it does not contain unresolved errors.

1.6
Checking RAID Configuration Status

Checking the RAID configuration status allows you to verify if the configuration is successfully completed.

Procedure:

1. Log on to Integrated Lights Out (iLO) with the **ilouser** user role.
2. From the left-hand menu, select **System Information**.
3. Select the **Storage** tab.
4. In the **Storage Information** section, perform the following actions:
   a. Select the **Logical View** radio button and verify if the **Controller Status** is `OK`.
   b. Verify if the **Cache Module Status** is `OK`.
   c. Verify if **Fault Tolerance** is set to: `RAID 1+0`.
   d. Select the **Physical View** radio button and verify if the **Controller Status** is `OK`.
   e. Verify if **Cache Module Status** is `OK`.

   The list of drives with their individual statuses is available under both **Logical View** and **Physical View**.

1.7
Configuring Time Synchronization

To configure time synchronization on all Standalone Authentication Centre Servers perform the following procedures:

Process:

1. Configuring Initial Time Service on page 26
2. Forcing Time Synchronization to the NTP Server on page 26
3. **New customers only:** If the time correction on iGAS was greater than 1 minute, reboot the server. See Rebooting the Physical Server on page 28.

1.7.1 Configuring Initial Time Service

Perform this procedure for all Standalone AuC Servers.

Prerequisites:

Log on to the server as **sysadmin** by using one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu ------------------------------ 1. Enable all
Application Servers 2. Disable all Application Servers 3. Display Status of all
Application Servers 4. Unix Administration 5. Application Servers Administration
Menus 6. Application Servers Boot/Reboot/Shutdown 7. Application Servers Status
Administration 8. Application Isolation Management Please enter selection (1-8, q)
[q]:
```

2. Enter the number for **Unix Administration**.

   The **Unix Administration** menu appears.

3. Enter the number for **NTP Administration**.

   The **NTP Administration** menu appears.

4. Enter the number for the **Display NTP status**.

   NOTE:
   If the NTP service is not started, select the **Disable NTP service** option, and then **Enable NTP service** option. Wait several minutes and check the NTP status again.

   For correct operation, NTP requires proper BIOS setup (date and time).

5. Enter the number for **Change NTP servers parameters**.

   The **NTP servers administration** menu appears.

6. Enter the number for **Set initial NTP servers configuration**.
7. At the warning message, enter: `y`

Result: The initial NTP configuration has been completed.
Postrequisites: Perform Forcing Time Synchronization to the NTP Server on page 26.

1.7.2 Forcing Time Synchronization to the NTP Server

Perform this procedure for all Standalone AuC Servers.

Prerequisites: Before performing this procedure make sure that you configured initial time service as described in Configuring Initial Time Service on page 26.

Log on to the server as `sysadmin`. Depending on the access method, see one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu ------------------------------ 1. Enable all
Application Servers 2. Disable all Application Servers 3. Display Status of all
Application Servers 4. Unix Administration 5. Application Servers Administration
Menus 6. Application Servers Boot/Reboot/Shutdown 7. Application Servers Status
Administration 8. Application Isolation Management Please enter selection (1-8, q)
[q]:
```

2. Type the number associated with **Unix Administration** and press **Enter**.

   The **Unix Administration** menu appears.

   ```
   Unix Administration ------------------- 1. Reboot physical server 2. Shutdown
   physical server 3. NTP Administration 4. Eject CD/DVD 5. Change password 6.
   Display IGAS version 7. Display server information Please enter selection (1-8, q)
   [q]:
   ```

3. Type the number associated with **NTP Administration** and press **Enter**.

   The **NTP Administration** menu appears.

   ```
   NTP Administration ------------------- 1. Enable NTP service 2. Disable NTP
   service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
   parameters 6. Change date and time Please enter selection (1-6, q) [q]:
   ```

4. Type the number associated with **Change NTP servers parameters** and press **Enter**.

   The **NTP servers administration** menu appears.

   ```
   NTP servers administration ------------------- 1. Set initial NTP servers
   configuration 2. Manage local clock 3. Manage primary NTP server 4. Manage
   secondary NTP server 5. Manage tertiary NTP server Please enter selection (1-5,
   q) [q]:
   ```

5. Perform one of the following actions:

   - If the local MSO includes the Network Time Server, type the number associated with **Manage primary NTP server**.
   - If the local MSO does not include the Network Time Server, type the number associated with **Manage secondary NTP server**.

   The NTP server menu appears. The below menu is an example of the primary server.

   ```
   NTP server: Primary ------------------- 1. Add server to list 2. Remove server
   from list 3. Show if server is on the list 4. Show server configuration 5. Update
   server configuration 6. Sync down time to this server Please enter selection (1-6,
   q) [q]:
   ```

6. Type the number associated with **Sync down time to this server** and press **Enter**.

   A number of messages appear finalized with:

   ```
   Do you really wish to continue? (y,n,q) [n]:
   ```

7. Type `y` and press **Enter**.

   The message about the successful time synchronization appears. Below is an example of an output:

   New customers:

   ```
   Restart Completed Time Sync Down successfully executed on iGAS. Time correction
   +0.010284 s. Time Sync Down successfully executed on hypervisor. Time correction
   -0.003540 s.
   ```

   Upgrading customers:

   ```
   Restarting CMA agent, please ignore interim UEM alarms for this IGAS and
   hypervisor Restart completed Time Sync Down successfully executed on iGAS. Time
   ```

```
correction +0.010284 s. Time Sync Down successfully executed on hypervisor. Time
correction -0.003540 s.
```

NOTE: Upgrading customers only: Upon successful time synchronization, CMA agent on IGAS restarts and transient alarms on UEM for synchronized host may appear. They should be ignored.

8. In the command line, type `q` and press ENTER until you get back to the **NTP Administration** menu.

   The **NTP Administration** menu appears:

   ```
   NTP Administration -------------------- 1. Enable NTP service 2. Disable NTP
   service 3. Display NTP status 4. Set NTP time zone 5. Change NTP servers
   parameters 6. Change date and time Please enter selection (1-6, q) [q]:
   ```

9. Type the number associated with **Enable NTP service** and press **Enter**.

   The **NTP Administration** menu appears.

Postrequisites:

New customers only: If the time correction on iGAS was greater than 1 minute, reboot the server. See Rebooting the Physical Server on page 28. Otherwise, go to iLO Configuration Verification on page 29.

Upgrading customers only: Continue to iLO Configuration Verification on page 29.

1.8 Rebooting the Physical Server

Prerequisites:

⚠ **CAUTION:** Rebooting the physical server can seriously disrupt system functionality. Do not attempt to reboot the server unless you are aware of all the system impacts.

Log on as **sysadmin** by using one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon, ensure that the **System Administrator Main Menu** appears.
2. Enter the number for **Unix Administration**.
3. Reboot the physical server by entering the number for **Reboot physical server**.

1.9 Configuring iLO Security

Procedure:

1. Log on to iLO with the **Administrator** user role.

If…	Then…
If you want to configure iLO 4 security,	perform the following actions: **a.** In the left-hand side panel, select **Administration** → **Security**. **b.** Select the **Encryption** tab. **c.** In the **Encryption Enforcement Settings** area, set the **Enforce AES/3DES Encryption** option to `Enabled`.
If you want to configure iLO 5 security,	perform the following actions: **a.** In the left-hand side panel, click **Security**. **b.** Select the **Encryption** tab. **c.** In the **Security Settings** area, set the **High Security** option.

2. Click **Apply**.

Result: The browser connection ends and the iLO interface restarts.

1.10 iLO Configuration Verification

1.10.1 Re-configuring iLO

NOTE: Perform the following procedure only in the case of unsuccessful server and iLO setup. Do not perform this procedure during regular server operation.

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu ------------------------------ 1. Enable all
Application Servers 2. Disable all Application Servers 3. Display Status of all
Application Servers 4. Unix Administration 5. Application Servers Administration
Menus 6. Application Servers Boot/Reboot/Shutdown 7. Application Servers Status
Administration 8. Application Isolation Management Please enter selection (1-8, q)
[q]:
```

2. Enter the number associated with **Unix Administration**.
3. In the **Unix Administration** menu, enter the number associated with **iLO administration**.
4. In the **iLO administration** menu, enter the number associated with **Reset iLO configuration**.

   NOTE: Resetting iLO may cause temporary alarm reports in UEM (Unified Event Manager). After a successful reset, the traps will be cleared.

   A number of system messages appear.

5. Reboot the server. See Rebooting the Physical Server on page 28.

Postrequisites:
Continue to one of the following:

- Go to Booting the Primary/Secondary Standalone AuC Server Application on page 30 if the last message from the previous step is:

  ```
  iLO set up successfully
  ```

- Go to Installing the iLO License on page 30 if the last message from the previous step is:

  ```
  iLO set up successfully (license not installed)
  ```

- Repeat the last step of this procedure if you get a message that the iLO configuration status is unknown.

1.10.2

Installing the iLO License

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

   ```
   System Administrator Main Menu ------------------------------ 1. Enable all
   Application Servers 2. Disable all Application Servers 3. Display Status of all
   Application Servers 4. Unix Administration 5. Application Servers Administration
   Menus 6. Application Servers Boot/Reboot/Shutdown 7. Application Servers Status
   Administration 8. Application Isolation Management Please enter selection (1-8, q)
   [q]:
   ```

2. Enter the number associated with **Unix Administration**.
3. In the **Unix Administration** menu, enter the number associated with **iLO administration**.
4. In the **iLO administration** menu, enter the number associated with **Install iLO license**.
5. At the prompt, enter the iLO license number that came with your server (only letters and numbers, without dashes).
6. Optional: If you receive a message stating that the scripting utility should be updated, disregard it.

Postrequisites: Continue to Booting the Primary/Secondary Standalone AuC Server Application on page 30 if the iLO license number was entered correctly or repeat the procedure if you get an error.

1.11

Booting the Primary/Secondary Standalone AuC Server Application

Prerequisites:
Reboot the server. Perform Rebooting the Physical Server on page 28.

Ensure that the Primary/Secondary Standalone AuC Server is already configured and holds the application licenses.

Log on to the server as `sysadmin`. Depending on the access method, see one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

   ```
   System Administrator Main Menu ------------------------------ 1. Enable all
   Application Servers 2. Disable all Application Servers 3. Display Status of all
   ```

```
Application Servers 4. Unix Administration 5. Application Servers Administration
Menus 6. Application Servers Boot/Reboot/Shutdown 7. Application Servers Status
Administration 8. Application Isolation Management Please enter selection (1-8, q)
[q]:
```

2. Type the number associated with **Application Servers Boot/Reboot/Shutdown** and press **Enter**.

   The **Application Servers Boot/Reboot/Shutdown** menu appears.

   ```
   Application Servers Boot/Reboot/Shutdown ----------------------------------------
   1. Boot Application Servers 2. Reboot Application Servers 3. Shutdown Application
   Servers Please enter selection (1-3, q) [q]:
   ```

3. Type the number associated with **Boot Application Servers** and press **Enter**.

   The **Boot Application** menu appears.

4. Type the number associated with **Boot all applications** and press **Enter**.

   All the application residing on the server boot.

1.12 Server Password Change

For security purposes, use the following guidelines when creating administrator passwords to ensure that they are difficult for unauthorized users to guess.

The password must meet the following criteria:

- At least 15 characters, containing elements from the four types of characters:
  1. English uppercase letters
  2. English lowercase letters
  3. Westernised Arabic numerals 0, 1, 2 … 9
  4. Special Characters !, @, #, $ …
- Differ from your logon name and any reverse or circular shift of your name
- Differ from the old password by at least three characters
- Have a minimum of eight different characters than old password
- Have no more than three consecutive repeating characters
- Have no more than four consecutive characters of the same class

⚠ **CAUTION:** The administrator password controls access to the administration menus. Keeping these menus secure is crucial, as the server's Administration menu provides access to vital network management functions. You should keep the administrator password secret and change it frequently.

1.12.1 Changing the Server Administrator Password

Perform this procedure to change the server administrator password.

NOTE: As a result of the following procedure, the iGAS `sysadmin` user passwords will be changed.

Prerequisites: Log on as `sysadmin` by using one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon as **sysadmin**, ensure that the **System Administrator Main Menu** appears.
2. Enter the number for **Unix Administration**.
3. Enter the number for **Change password**.
4. At the prompt, enter the current password.
5. At the prompt, enter the new password.
6. Enter the new password again.

   A message appears stating that the password was changed successfully and you are returned to the previous menu.

   NOTE: If the second password does not match the first, an error message appears, and you are returned to the previous menu.

1.12.2 Changing the iLO User Password

Procedure:

1. Log on to iLO as the Administrator.
2. In the panel on your left-hand side, select **Administration** → **User Administration**.
3. In the **Local Users** section, select the check box next to the user whose password you want to change and click **Edit**.
4. In the **User Information** section, select the **Change password** check box if needed.
5. Type the new password in the **Password** and **Password Confirm** fields and click **Update User**.

   NOTE: It is not recommended to use the = sign when setting the iLO password.

1.13 Configuring the Primary/Secondary Standalone AuC Server Application

1.13.1 Installing the External Modem Driver for KVL to AuC/PrC Communication

Perform this procedure if you use the AuC/PrC to KVL modem connection. Otherwise, skip to the next one.

If you use the StarTech USB56KEMH2 modem, Windows automatically configures the connection. See: “Configuring KVL Port Settings” in the *Authentication Centre (AuC) User Manual*. The modem should be attached and detached in `out of service` or `disabled` server mode.

This procedure can be performed only by members of the Administrators group.

Procedure:

1. Stop the AuC/PrC services:

   a. As an Administrators group member, on the AuC/PrC desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

   b. In the **Config Assistant** window, enter: `ca disable`

2. Open **Control Panel** .
3. In the **All Control Panel Items** window, select **Phone and Modem**.
4. If the **Location Information** window appears, enter the required information and click **OK**.
5. In the **Phone and Modem** window, select the **Modems** tab.
6. Click **Add**.
7. In the **Add Hardware Wizard** window, select the **Don't detect my modem; I will select it from a list** check box. Click **Next**.
8. Select **Have Disk**.
9. In the **Install From Disk** dialog box, select **Browse**.
10. Perform one of the following actions:
    - If you use the MT5656ZDX modem, navigate to `C:\Motorola\AuC\`*`<version>`*`\drivers\modem\MT5656ZDX\5656.INF`, and click **Open**.
    - If you use the old MT9234ZBA modem, navigate to `C:\Motorola\AuC\`*`<version>`*`\drivers\modem\MT9234ZBA\MultitechA.INF`, and click **Open**.
11. In the **Install From Disk** dialog box, click **OK**.
12. From the **Models** list, select one of the following:
    - If you use the MT5656ZDX modem, select **MultiTech Systems MT5656ZDX**. Click **Next**.
    - If you use the old MT9234ZBA modem, select **MultiTech MT9234ZBA**. Click **Next**.
13. Ensure that the **Selected ports** radio button is selected, and perform one of the following actions:
    - For AuC, select **COM1** and click **Next**.
    - For PrC, select **COM2** and click **Next**.

    The installation process starts, followed by the confirmation message.
14. Click **Finish**.
15. Start the AuC/PrC services:

    a. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

    b. In the **Config Assistant** window, enter: `ca enable`

Postrequisites: Ensure that the KVL ports are correctly configured. See "Configuring KVL Port Settings" in the *Authentication Centre (AuC) User Manual*, or *Clear Authentication Centre (AuC) User Manual*.

Related Links

Primary/Secondary AuC Standalone Server Application Restoration on page 35

1.14 Installing and Configuring RSA Authentication Software

Procedure:

1. If RSA Two-Factor Authentication is present in the system, clear 2FA Secret key on the RSA server for each application server that was installed on the Standalone AuC Server. Follow the “Clearing the Node Secret for a Particular Node” procedure in the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.

   IMPORTANT:
   When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

   The RSA Agent installation should be performed after the promoting of Domain Controller.

1.15 Accessing Hypervisor Web-Based Console

NOTE: In Dimetra 9.1.1, hypervisor web-based console can be used to access system performance statistics, view the list of services running on hypervisor with their statuses, and access the sysadmin menu through the terminal. To access the web-based console, you should use sysadmin credentials.

Procedure:

1. Log on to the Network Management Terminal (NMT) computer.
2. Open a web browser (Chromium).
3. In the address field, enter the IP address of the HostOS you want to access.
4. Perform the following actions:
   a. In the **User name** field, enter: `sysadmin`
   b. In the **Password** field, enter the password.
   c. Click **Log in**.

Chapter 2

Primary/Secondary AuC Standalone Server Application Restoration

Table 3: AuC – Restoration References

Action	Reference	Done
AuC Restoration	AuC – Restoration Impact on page 35	
	AuC – Pre-Restoration Checks on page 36	
	AuC – Restoring Application on page 40	
	AuC – Restoring Data from Backup on page 42	
	AuC – Configuring Application on page 47	
	AuC – Post-Restoration Checks on page 52	
	AuC – Installing and Configuring RSA Authentication Software on page 52	
AuC Database Restoration	AuC – Restoration Impact on page 35	
	AuC – Pre-Restoration Checks on page 36	
	AuC – Restoring Data from Backup on page 42	
	AuC – Configuring Application on page 47	
	AuC – Installing and Configuring RSA Authentication Software on page 52	
	AuC – Post-Restoration Checks on page 52	
Replacing AuC CryptR2	AuC – Restoration Impact on page 35	
	AuC – Pre-Restoration Checks on page 36	
	Replacing CryptR2 on page 44	
	AuC – Post-Restoration Checks on page 52	

2.1 AuC – Restoration Impact

Table 4: AuC – Restoration Impact

Action	Service Affected	Service Downtime
AuC container restoration	● No distribution of keys and authentication material. ● No updates of keys and authentication material.	Approximately 30 minutes, depending on the size of database

Table continued…

Action	Service Affected	Service Downtime
AuC database restoration	● No distribution of keys and authentication material. ● No updates of keys and authentication material.	Approximately a couple of minutes, depending on the size of database
CryptR2 replacement	● No distribution of keys and authentication material. ● No updates of keys and authentication material.	Approximately 0.5 hour

Related Links

Primary/Secondary AuC Standalone Server Application Restoration on page 35

2.2
AuC – Pre-Restoration Checks

Table 5: AuC – Pre-Restoration Checks

Action	Pre-Restoration Checks
All restoration procedures	Back up the database (if possible). Check statuses of the: UCS, ZDSs - for more information, see the *Network Management Servers* manual. - base sites on the AuC Client, if available. Alternatively, use UEM/System Health Application Suite.
	Determine Key Version Numbers in AuC Backup File.

2.2.1
AuC - Checking Status of the

Prerequisites:
Log on to the server as **sysadmin** by using one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. At logon as **sysadmin**, verify that the **System Administrator Main Menu** appears:

```
System Administrator Main Menu ------------------------------ 1. Enable all
Application Servers 2. Disable all Application Servers 3. Display Status of all
Application Servers 4. Unix Administration 5. Application Servers Administration
Menus 6. Application Servers Boot/Reboot/Shutdown 7. Application Servers Status
Administration 8. Application Isolation Management Please enter selection (1-8, q)
[q]:
```

2. Enter the number associated with **Application Servers Administration Menus**.

   The **Application Servers Administration Menus** list appears.

   NOTE: The list of available application servers varies depending on the Server type.

3. Enter the number associated with .

   The login prompt appears.

4. Log on as `szadmin`.

   The application server displays initial administrative prompts.

   NOTE: The initial administrative prompts vary depending on the application server in question.

5. Press Enter to close the initial prompt.

   You are logged on, and the **System Administration** menu appears.

6. Enter the number for .
7. Enter the number for **Check System Status**.

   The System status information appears. Example messages is shown below:

   ```
   The Zone Controller status is: ENABLED_ACTIVE. The Database Server status is:
   ENABLED. The Zone Controller operating mode is: INTEGRATED. The Zone Controller
   requested status is: ENABLE.
   ```

8. Verify that the active shows `ENABLED_ACTIVE`.

2.2.2 AuC - Recording the Key Version Numbers

Procedure:

1. Launch the AuC client.
2. Log on as a valid user with appropriate permissions.
3. From the toolbar, select **System** → **Go Out of Service**.

   The event is logged in the **Events** window.

4. Open the **Devices** tab.
5. Record the KEKm, KEKz, CCK, and SCK Present and Future Key Version Numbers for the Zone as reported on the AuC Client.

2.2.3 AuC - Determining Key Version Numbers in AuC Backup File

Procedure:

1. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
2. Perform one of the following actions:

- To display information about key version numbers for the currently used database, enter: `ca keysreport`
- To display information about key version numbers from the backup file, enter: `ca keysreport -i <backup file name>`

Keys version report is displayed in the **CA** window.

3. Make notes of all Key Version numbers or, if possible, print the file.
   - If the AuC database contains higher versions of the keys than are actually loaded on Zone Controllers and Sites, continue.

     In this case, AuC aligns the keys to the correct versions.
   - If the keys are otherwise not aligned, contact Motorola Solutions support for advice on how to manually synchronize keys.

Related Links

Primary/Secondary AuC Standalone Server Application Restoration on page 35

2.2.4 AuC – Managing AuC Roles

Configuration Assistant tool is used to check and change AuC server current role.

It is possible to check AuC current role, change role from Active to Standby and the other way around.

2.2.4.1 Switching the Roles of the AuC Servers

If the server role is UNKNOWN, Config Assistant tries to set the role requested by the user.

Config Assistant does not proceed with changing role if network setup is incorrect (unknown IP address – not following the IP plan).

Procedure:

1. Log on to the Active AuC.
2. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

   Config Assistant window opens.
3. Enter: `ca role standby`
4. Enter: `y`

   The following message appears:

   ```
   Changing application role to STANDBY...
   ```
   then the Active AuC will be shut down.
5. Permanently shut down AuC by following procedure: Shutting Down Application Servers

   NOTE: After the virtual machine is shut down, iGAS automatically attempts to restart the application, which can lead to IP conflict.
6. Log on to the Standby AuC.

7. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

   Config Assistant window opens.

8. Enter: `ca role active`

   You are asked to confirm the operation.

9. Enter: `y`

   The following message appears:

   ```
   Changing application role to ACTIVE...
   ```

   It can take some time till the action is finished, then the server will be rebooted.

10. Log on to the Core Server's iGAS administration menu and boot the standby AuC. See the *Network Management Servers* manual.

2.2.4.2 Managing AuC Roles After Failure of Active AuC

IMPORTANT: To avoid possible IP conflicts, make sure that active AuC is shut down before proceeding with the activation procedure.

In case of failure of the AuC server, you need to change the role of the Standby AuC server to became Active. In such a case:

- Verify **Data currency** using Standby Manager GUI Client:

  IMPORTANT: If both values displayed in **Last synchronized** and **Last changes applied** fields are **None** do not proceed with changing roles but reinstall Active_AuC and restore from backup file.

  NOTE: Before proceeding with activation procedure consider data currency of the standby AuC (more recent date from **Last synchronized** and **Last changes applied** fields on Standby GUI Client). If you have newer backup file – reinstall active AuC and restore from that backup file.

- Change the role of the AuC B server (from Standby to Active) as per Changing the Role of the Standby AuC to Active AuC on page 39.
- Perform required repairs to the damaged AuC A server
- On AuC A install AuC as Standby (choose the Standby option while installing AuC software)

To restore the original state (AuC A = Active, AuC B = Standby), perform Switching the Roles of the AuC Servers on page 38.

2.2.4.3 Managing AuC Roles After Failure of Standby AuC

In case of failure of the Standby AuC server, reinstall the server from iGAS menu selecting standby option while reinstalling. You need to boot standby AuC from iGAS menu after the installation is finished. Database Standby manager is operating.

2.2.4.4 Changing the Role of the Standby AuC to Active AuC

Procedure:

1. Log on to the Standby AuC using the following IP address: `10.0.<ClusterOctet>.220`

2. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.

   Config Assistant window opens.

3. Enter: `ca role active`.

   You are asked to confirm the operation.

4. Enter: `y`

   The following message appears:

   ```
   Changing application role to ACTIVE...
   ```

   It can take some time till the action is finished, then the server will be rebooted.

2.3 AuC – Restoring Application

Prerequisites: Log on to the server as **instadm**. Depending on the access method, see one of the following procedures:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. Enter the number for **Reinstall Applications**.

   The list of available applications residing on the server appears.

2. Enter: `y` when the installer prompts you to re-install Authentication Centre and enter: `n` for other applications.

   The following message appears:

   ```
   Please select AUC role: 1. Active 2. Standby
   ```

3. Enter the number reflecting the AuC role in the system.

   The following message appears:

   ```
   Disable the PrC functionality on the Enhanced AuC (y,n) [n]?
   ```

4. Enter: `y` or `n` accordingly.

   The re-installation process starts. When the re-installation is complete, the **Installation Administrator Main Menu** appears.

5. Log off from the server by entering: `q`
6. Log on to the server using **sysadmin** login and password.

   The **System Administrator Main Menu** appears.

7. Enter the number for **Application Servers Boot/Reboot/Shutdown**.

   The **Application Servers Boot/Reboot/Shutdown** menu appears.

8. Enter the number for **Boot Application Servers**.
9. Enter the number for Authentication Centre.

   You have booted the application.

10. Enter: `q` and repeat this sequence until you log off from the server.

Related Links

Primary/Secondary AuC Standalone Server Application Restoration on page 35

2.3.1 Installing the External Modem Driver for KVL to AuC/PrC Communication

Perform this procedure if you use the AuC/PrC to KVL modem connection. Otherwise, skip to the next procedure.

This procedure can be performed only by members of the Administrators group.

If you use the StarTech USB56KEMH2 modem, Windows automatically configures the connection. See "Configuring KVL Port Settings" in the *Authentication Centre (AuC) User Manual*. The modem should be attached and detached in `out of service` or `disabled` server mode.

Procedure:

1. Stop the AuC/PrC services:
   a. As an Administrators group member, on the AuC/PrC desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
   b. In the **Config Assistant** window, enter: `ca disable`
2. Open **Control Panel** .
3. In the **All Control Panel Items** window, select **Phone and Modem**.
4. If the **Location Information** window appears, enter the required information and click **OK**.
5. In the **Phone and Modem** window, select the **Modems** tab.
6. Click **Add**.
7. In the **Add Hardware Wizard** window, select the **Don't detect my modem; I will select it from a list** check box. Click **Next**.
8. Select **Have Disk**.
9. In the **Install From Disk** dialog box, select **Browse**.
10. Perform one of the following actions:
    - If you use the MT5656ZDX modem, navigate to `C:\Motorola\AuC\`*`<version>`*`\drivers\modem\MT5656ZDX\5656.INF`, and click **Open**.
    - If you use the old MT9234ZBA modem, navigate to `C:\Motorola\AuC\`*`<version>`*`\drivers\modem\MT9234ZBA\MultitechA.INF`, and click **Open**.
11. In the **Install From Disk** dialog box, click **OK**.
12. From the **Models** list, select one of the following:
    - If you use the MT5656ZDX modem, select **MultiTech Systems MT5656ZDX**. Click **Next**.
    - If you use the old MT9234ZBA modem, select **MultiTech MT9234ZBA**. Click **Next**.
13. Ensure that the **Selected ports** radio button is selected, and perform one of the following actions:
    - For AuC, select **COM1** and click **Next**.
    - For PrC, select **COM2** and click **Next**.

    The installation process starts, followed by the confirmation message.

14. Click **Finish**.
15. Start the AuC/PrC services:
    a. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
    b. In the **Config Assistant** window, enter: `ca enable`

Postrequisites: Ensure that the KVL ports are correctly configured. See “Configuring KVL Port Settings” in the *Authentication Centre (AuC) User Manual*.

2.4 AuC – Restoring Data from Backup

2.4.1 AuC - Starting Up the Upgrade Console

Prerequisites: Log on to the NM Client PC.

Procedure:

1. Open a web browser (Chromium) and enter the following URL address: `https://master-uis.ucs/ui`
2. In the **User name** field, enter a user name associated with the **Backup** user role.
3. In the **Password** field, enter the password associated with the user.
4. Click **Log in**.

   You are logged on to the Upgrade Console and connected to the Master UIS. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

Postrequisites: If you need to upload the backup file from the NM Client PC to the UIS, continue to AuC – Uploading a Backup File to UIS on page 42, otherwise if the backup file already is in the UIS backup storage, log on to the server.

2.4.2 AuC – Uploading a Backup File to UIS

Prerequisites: Log on to the Upgrade Console with the **Backup** user role.

Ensure that a data backup file is available on the NM Client PC from which you have launched the Upgrade Console.

Upload the data backup file to the UIS backup storage, so that you can use it for data restoration.

NOTE: If you have already stored the required backup file in the UIS backup storage, you can skip this procedure.

Procedure:

1. In the menu at the left side of the Upgrade Console, select **Upload Files**.

   The **Upload Files** screen appears.

2. Click **Browse**.

3. In the window that appears, select your backup file. Click **OK**.

   NOTE: The backup file is named `cluster`*<XX>*`_aucdb_01_`*<timestamp>*, where *<XX>* is the cluster ID, and *<timestamp>* is a date and time written as one row of digits with the format *<yyyymmddhhmm>*.

   The name of the selected file appears in the **File Name** field.

4. Click **Upload**.
5. Click **Analyze Uploaded File**.

   If the file format is correct, the file is placed in the backup storage of the UIS to which you are connected. The backup file may be placed either on the Master UIS (which is a central backup storage) or on the Home UIS for the particular application.

2.4.3 AuC – Disabling the Application Server

Prerequisites: Log on to iGAS as **sysadmin** by performing one of the following actions:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. Enter the number for **Application Servers Status Administration**.
2. Enter the number for **Disable Application Servers**.
3. Enter the number for the server that you want to disable.
4. At the confirmation prompt, enter: `y`

   A message appears showing that the application server is disabled.

5. Enter: `q` twice to go back to the **Application Servers Status Administration** menu.

2.4.4 AuC – Restoring Data from Backup

Prerequisites:
You must be logged on to the Upgrade Console on the Master UIS, with the **Backup** user role. A data backup file must be available. The application server that you want to restore must be disabled. If the application server is enabled, the restoration fails.

Procedure:

1. From the menu on the left side of Upgrade Console, select **Restore**.

   A table appears, showing available backup files for applications in the different zones.

2. Click **Refresh File name**.

   The file names of the backup files are read on the default storage for each application.
   If you previously configured usage of central storage for the backup, the default Storage is Master UIS. Otherwise, it is Zone UIS. If you configured usage of a Storage PC, then a list of backup file names stored on Storage PCs will be available. **Last refresh on** shows a time stamp for the last time a file name refresh was carried out.

3. In the **Backup File name** column, from the drop-down list, select the appropriate backup file.
4. In the **Action** column for the backup file and application, click **Run**.

   NOTE: The backup file is named `cluster`*<XX>*`_aucdb_01_`*<timestamp>*, where *<XX>* is the cluster ID, and *<timestamp>* is a date and time written as one row of digits with the format *<yyyymmddhhmm>*.

   A message appears prompting you to decide whether you want to restore data.

5. Click **Yes**.

   An indicator shows that the restoration task is running. The **Restore Status** column shows that the restoration task has started, and it shows when the task has been completed.

   NOTE: The backup file names are used during the restoration task. If the backup file name on the default storage has changed since the last refresh, the restoration task fails.

2.4.5
AuC – Enabling the Application Server

Prerequisites: Log on to iGAS as **sysadmin** by performing one of the following actions:

- Logging On to the Server on page 22
- Logging On to iGAS Through a KVM Switch on page 24

Procedure:

1. Enter the number for **Application Servers Status Administration**.
2. Enter the number for **Enable Application Servers**.
3. Enter the number for the application server you want to enable.

   A message appears showing that the application server is enabled.

4. Enter: `q` twice to go back to the **Application Servers Status Administration** menu.

Related Links

Primary/Secondary AuC Standalone Server Application Restoration on page 35

2.5
Replacing CryptR2

Procedure:

1. From NM Client, connect to the AuC server using the Remote Desktop.
2. Start the **Enhanced Authentication Centre Client**.
3. From the **System** menu, select **Go Out Of Service**.

   The **Enhanced Authentication Centre Client** reports the `Out of Service state` of the server.

4. Disconnect the damaged CryptR2.
5. Configure the new CryptR2 device (IP and passwords) and connect it. For more information on setting up CryptR2, see the *Authentication Centre (AuC) User Manual*.
6. Load the CryptR2 Master Keys using KVL. See Loading Keys with KVL on page 45.

Postrequisites: To verify that you replaced the CryptR2 device correctly, see "Verifying DVI-XL Master Keys" in the *Authentication Centre (AuC) User Manual*.

2.5.1 Loading Keys with KVL

Procedure:

1. In the Authentication Centre (AuC) Client, from the **System** drop-down menu, select **Encryption Devices**.

   The client displays the encryption device with a status of `Not Loaded`.

2. In the **Encryption Device** window, click **Enter Password** and enter passwords for admin and user accounts.
3. Validate the passwords by clicking **Validate**.
4. Click **Enter AES Master Key** and enter the key. Click **OK**.
5. Click **Load Master Key** and select the DVI-XL key and KVL interface.
   1. After clicking through the informational messages, the AuC Client allows one minute to use the KVL to load the master key.
   2. Using the key loading cable connect the KVL to the CryptR2.
   3. From the main menu, select **Crypto Device** on the KVL.
   4. From the list of available Master Keys, select a DVI-XL key to be loaded into the Crypto Device.

      WARNING: This must be the same DVI-XL Master Key as previously loaded, including the same DVI-XL system key associated to the Master Key. If you change the Master Key, all provisioning related to the Air Interface Encryption infrastructure and radios requires re-provisioning from scratch. For more information, see the *Authentication Centre (AuC) User Manual* or *Clear Authentication Centre (AuC) User Manual*.

      A message appears confirming that the operation was successful.

6. In the **Encryption Device** window, click **Load Master Key** and select AES key and KVL interface.
   1. After clicking through the informational messages, the AuC Client allows one minute to use the KVL to load the master key.
   2. From the main menu, select **Crypto Device** on the KVL.
   3. From the list of available Master Keys, select AES 128 key to be loaded into the Crypto Device.

      A message appears confirming that the operation was successful.

7. Return to the AuC Client.
8. From the main AuC Client menu, select **System** → **Go Operational**.

2.5.2 Loading Keys with Serial Connection

Procedure:

1. Open the **Enhanced Authentication Centre Client**. From the **System** drop-down menu, select **Encryption Devices**.
2. The **Enhanced Authentication Centre Client** displays the encryption device with a status of **Not Loaded**.

3. In the Encryption Device window, click **Enter Password** button, then enter passwords for admin and user accounts.
4. Click **Validate** button, to validate the passwords.
5. Click **Enter AES Master Key** button, then enter and confirm the key and click **OK**.
6. Click **Load Master Key** button, then select DVI-XL key and serial interface.
   a. Once the informational messages have been clicked through, the **Enhanced Authentication Centre Client** allows one minute to use the serial connection to load the master key.
   b. Using the USB to Mini USB cable connect the service laptop to the CryptR2.
   c. Establish a serial connection between the service laptop and CryptR2 using Com*<X>* port, where *<x>* is the serial port assigned to CryptR2. Use the following settings:
      - Baud rate: **9600**
      - Parity: **none**
      - Data bits: **8**
      - Stop bits: **1**

   d. Log on as **user**

      The `mkload>` prompt appears. You are prompted to enter the first master key.

   e. Enter the first master key consisting of 128 hexadecimal digits.

      You are prompted to enter the second master key.

   f. Enter the second master key consisting of 16 hexadecimal digits.

      A message confirming that the operation was successful appears.

   g. Press ENTER.
   h. Return to the **Enhanced Authentication Centre Client**.

      Once the master key is loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.

   i. Click **OK**.
7. In the Encryption Device window, click **Load Master Key** button, then select AES key and serial interface.
   a. Once the informational messages have been clicked through, the **Enhanced Authentication Centre Client** allows one (1) minute to use the serial connection to load the master key.
   b. Log on as **user**

      The `mkload>` prompt appears. You are prompted to enter the master key.

   c. Enter the master key consisting of 32 hexadecimal digits.

      A message confirming that the operation was successful appears.

   d. Return to the **Enhanced Authentication Centre Client**.

      Once the master key is loaded, the **Enhanced Authentication Centre Client** displays a confirmation that the operation was successful.

e. Click **OK**.

⚠ **WARNING:** This must be the same Master Key as stored in the **Enhanced Authentication Centre Client** Database. If you change the Master Key, all provisioning related to the Air Interface Encryption infrastructure and radios requires re-provisioning from scratch. For more information, see the *Authentication Centre (AuC) User Manual* manual.

8. Return to the **Enhanced Authentication Centre Client** and perform the following actions:

   a. From the main menu, select **System**.

   b. Select **Go Operational**.

2.6 AuC – Configuring Application

2.6.1 AuC – Restoring Keys After a Database Restore

This section describes restoring keys after a database restore. The following scenarios are covered:

- AuC – Restoring Keys on a Single Cluster AuC on page 47 – follow this procedure if you are restoring a single cluster AuC.
- AuC – Restoring Keys on a Master AuC on page 48 – follow this procedure if you are restoring a master AuC.
- AuC – Restoring Keys on a Slave AuC on page 49 – follow this procedure if you are restoring a slave AuC.

2.6.1.1 AuC – Restoring Keys on a Single Cluster AuC

Procedure:

1. Open the Authentication Centre client.

   The configuration wizard appears.

2. In the **Confirm nationwide settings** window, select the **data is correct** radio button and click **Next**.
3. In the **Choose restoration type** window, select the **AuC will update (if necessary) keys in the system** radio button and click **Next**.
4. In the **Apply settings** window, set the `<Comm Key>` and `<Threshold>` values and confirm your settings by clicking the **Apply settings** button.

   NOTE:
   The Comm Key setting is not needed for the single cluster configuration.

   The Threshold (Sites) value is set to 100% by default.

5. Click **Finish**.

   NOTE:
   Zone Controllers and BTSs connect to the Authentication Centre and report the version of keys they possess. It is illustrated in the **Max reported by device** field.

   When the threshold is reached, you can check the versions of keys proposed by AuC.

   The AuC client window appears with the **Restoring** tab opened.

A `Restore in progress - threshold not met` information is displayed in the **Restore Statistics** group.

6. Wait until the `Restore in progress - threshold met` confirmation appears in the **Restore Statistics** group.

   The restoration process is completed.

   NOTE: If any problems with CMG configuration are reported on this tab, contact Motorola Solutions support for further assistance.

7. From the right-hand side of the **Restore Statistics** group, click the **Align keys** button.
8. In the **Confirmation** dialog box, click **OK**.

   AuC begins the alignment of keys in the system.

9. Perform one of the following actions:
   - If the **OTAR keys clearance confirmation** dialog box appeared, proceed to AuC – Restoring Keys Troubleshooting on page 50.
   - If the **OTAR keys clearance confirmation** dialog box did not appear, proceed to AuC – Post-Restoration Checks on page 52.

2.6.1.2 AuC – Restoring Keys on a Master AuC

Procedure:

1. Open the Authentication Centre client on the restored Master AuC.

   The nationwide settings configuration wizard appears.

2. In the **Confirm nationwide settings** window, select the **data is correct** radio button and click **Next**.
3. In the **Choose restoration type** window, select the **AuC will update (if necessary) keys in the system** radio button and click **Next**.
4. In the **Apply settings** window, set the **Comm Key** and **Threshold** values and confirm your settings by clicking the **Apply settings** button.

   NOTE:
   If backup contains outdated Comm Key material, set up a new Comm Key.

   The Threshold (Sites) value is set to 100% by default.

   A status message about connection of slave AuCs appears.

5. Wait until the message disappears and click **Finish**.

   NOTE:
   The AuC waits for all slave AuCs to connect for maximum 5 minutes.

   - If no un-restored slave AuCs connected during this time, a failure message is displayed and the AuC will hang until at least one of the un-restored slave AuCs connect.
   - If one or more un-restored slave AuCs connected during this time, the AuC client window with the **Restoring** tab appears. A `Restore in progress - threshold not met` information is displayed in the **Restore Statistics** group.

6. Wait for a `Restore in progress - threshold met` confirmation in the **Restore Statistics** group.

7. Click the **Accept Nationwide keys** button.

   IMPORTANT:
   Check all key versions which are proposed in **New Target** column and compare them to the key versions in **Max reported by devices** column.

   If differences are found in CMG keys (GCK, TM-SCK, DM-SCK, GSKO) it is recommended to contact Motorola Solutions support to evaluate possible consequences of accepting these keys. It might be the case that changing security class will be needed for such situation in a whole system.

8. In the **Confirmation** dialog box, click **OK**.

   The keys restoration process is completed. The AuC client launches.

9. Perform one of the following actions:

   - If the **OTAR keys clearance confirmation** dialog box appeared, proceed to AuC – Restoring Keys Troubleshooting on page 50.
   - If the **OTAR keys clearance confirmation** dialog box did not appear, proceed to AuC – Post-Restoration Checks on page 52.

2.6.1.3 AuC – Restoring Keys on a Slave AuC

Procedure:

1. Open the Authentication Centre client on the restored machine.

   The nationwide settings configuration wizard appears.

2. In the **Confirm nationwide settings** window, select the **data is correct** radio button and click **Next**.
3. In the **Choose restoration type** window, select the **AuC will update (if necessary) keys in the system** radio button and click **Next**.
4. In the **Apply settings** window, set the **Comm Key** and **Threshold** values and confirm your settings by clicking the **Apply settings** button.

   NOTE:
   If backup contains outdated Comm Key material, set up a new Comm Key.

   The Threshold (Sites) value is set to 100% by default.

   A status message about the connection to the Master AuC appears.

5. After the connection with master AuC is established click the **Finish** button.

   The AuC client window with the **Restoring** tab opened appears.

   A `Restore in progress - threshold not met` information is displayed in the **Restore Statistics** group.

6. Wait for a `Restore in progress - threshold met` confirmation in the **Restore Statistics** group.

7. Click the **Accept Nationwide keys** button.

   IMPORTANT:

   Check all key versions which are proposed in **New Target** column and compare them to the key versions in **Max reported by devices** column.

   If differences are found in CMG keys (GCK, TM-SCK, DM-SCK, GSKO) it is recommended to contact ESSC to evaluate possible consequences of accepting these keys. It might be the case that changing security class will be needed for such situation in a whole system.

8. In the **Confirmation** dialog box, click **OK**.

   The keys restoration process is completed. The AuC client launches.

9. Perform one of the following actions:

   - If the **OTAR keys clearance confirmation** dialog box appeared, proceed to AuC – Restoring Keys Troubleshooting on page 50.
   - If the **OTAR keys clearance confirmation** dialog box did not appear, proceed to AuC – Post-Restoration Checks on page 52.

2.6.1.4

AuC – Restoring Keys Troubleshooting

During the process of key alignment, the following scenarios may appear:

- GSKO has advanced in crypto period and at least one depending key has also advanced in crypto period, compared to the keys in the backup.
- GSKO is identical to the GSKO in the backup, but GCK and possible TM-SCK or DM-SCK keys have advanced in crypto period.

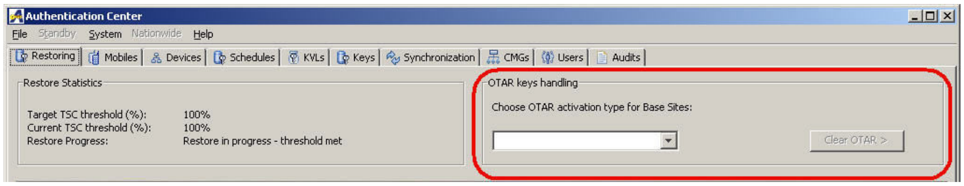
If the system is in SC3G then sites fallback to SC3 until the key restoration process is completed.

Procedure:

1. In the **OTAR keys clearance confirmation** dialog box, click **OK**.

   The **OTAR keys handling** group appears in the upper right-hand corner of the **Restoring** tab.

   Figure 2: OTAR Keys Handling Group Box

   Target TSC threshold (%): 100%
   Current TSC threshold (%): 100%
   Restore Progress: Restore in progress - threshold met

   Choose OTAR activation type for Base Sites:

   NOTE: You can monitor the tasks AuC is performing during the process of key alignment in the **Restore Statistics** group.

2. In the **OTAR keys handling** group, from the drop-down menu, select the preferred activation method.

   NOTE: For illustrative purposes, the Manual type of activation is detailed in the next steps of this procedure. This type of activation demands the user to trigger the OTAR activation manually.

   Once the OTAR activation type is selected, the **Clear OTAR** button (located next to the drop-down menu) becomes active.

3. Click the **Clear OTAR** button.

4. In the **Restore stage confirmation** dialog box, click the **Yes** button.

   Authentication Centre determines whether only the GCK keys, or the GCK, TM-SCK, and DM-SCK keys need clearing in the Base Sites. The application demands actions from the user accordingly.

5. Optional: If AuC clears only the GCK keys, then wait for the GCK threshold for Base Sites to be reached and proceed to step 8.

   NOTE:
   You can expedite the restoration by pressing the **Send OTAR** / **Send GSKO** button, but this does not speed up the key synchronization process.

   You can repeat this action for all types of keys.

   AuC clears the OTAR GCK keys in Base Sites.

6. Wait for the threshold for Base Sites to be reached.

   AuC is clearing OTAR GCK, TM-SCK, DM-SCK keys in Base Sites.

7. Wait for the OTAR GSKO threshold for Mobile Stations to be reached.

   AuC sends OTAR GSKO keys to Zone Controllers.

8. Wait for the OTAR GCK threshold for Mobile Stations to be reached.

   NOTE: During the Manual restoration, click the **Activate OTAR** button to finish the process (irrespective of whether the threshold was reached, or not).

   OTAR is activated, the key restoration process is completed and support for SC3G is restored.

   The **AuC Restoring** tab disappears.

2.6.2 AuC – Ensuring That AuC Is Operational After Restoration

Procedure:

1. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
2. Enter: `ca status -v` and verify if AuC services are running. If not, enter: `ca enable` to start them.
3. Log on to the AuC Client.
4. Ensure that CryptR2 has been detected and is usable. From the main menu, select **System** → **Encryption Device**.

   The device status must be `Working`. If the status is different, the problem **must** be resolved before proceeding.

   NOTE: The possible causes of CryptR2 failure are as follows:

   - No Master Key is loaded into CryptR2
   - Windows driver for CryptR2 is not installed
   - CryptR version is incorrect

5. Ensure the AuC operational state is set to **Operational**.

   NOTE: If the AuC operational service is **Out of Service**, from the main menu select **System Go Operational**.

Related Links

Primary/Secondary AuC Standalone Server Application Restoration on page 35

2.6.3 AuC – Cleaning Up the AuC Database

Procedure:

1. As an Administrators group member, on the desktop, right-click the **Config Assistant** icon and select **Run as administrator**.
2. Enter: `ca disable`
3. Enter: `ca enable -d`
4. Enter: `ca dbreset`

   You are prompted to confirm the command.
5. Enter: `y`

   Wait while the database is cleaned up. Command prompt appears.
6. Close **Config Assistant** window.

Result:

NOTE: After performing this procedure, AuC looks like only just installed application and requires configuration.

2.7 AuC – Installing and Configuring RSA Authentication Software

Procedure:

1. Clear 2FA Secret key on the RSA server. See the *Network Security* manual.
2. Install and configure the RSA software. For more information, see the *Network Security* manual.

   IMPORTANT:
   When restoring a physical server that hosts multiple virtualized applications, RSA software should be installed on each Windows application separately.

   The RSA Agent installation should be performed after the promoting of Domain Controller.

2.8 AuC – Post-Restoration Checks

Table 6: AuC – Post-Restoration Checks

Action	Post-Restoration Checks
AuC restoration - all procedures	Check if the UCS and ZDSs are connected. Use the **Synchronization** tab on the AuC Client.

Table continued…

Action	Post-Restoration Checks
	Check statuses of ZCs and base sites. Use the **Devices** tab on the AuC Client.
	Check in the **Schedules** tab that active and inactive keys are as expected.
	At a time agreed with users, ensure at least two key updates are successful.
	Check that AuC is highlighted green and has an `OK` status in UEM.

2.9

AuC – Backup Procedures

A user that has database management permissions can start a backup on demand from the AuC client.

Be aware of available disk space and remove old backups when no longer needed. Single backup can take ~0.5GB - so if old backups are not deleted they can use all available disk space.

NOTE:

Scheduled backup, if started in the middle of important action (like key updates, CMG edits, etc) will not be very useful. Manual backups should be executed when the AuC database in stable state.

You must log on the NM Client as **motosec** user in order to be able to connect to the AuC Server.

Before starting backup ensure that AucPgSvcR09xxxxx service is running using the `ca status -v` command form the **Config Assistant** tool, which needs to be opened by an Administrators group member by using the **Run as administrator** option.

2.9.1

AuC - Backing up Data

A data backup must be created regularly according to the backup frequency defined for the application. You can make a backup on-demand, or you can set up a scheduled backup that runs automatically at regular intervals. Before you can create the backup, you need to configure it.

2.9.1.1

AuC - Starting Up the Upgrade Console

Prerequisites:

Before you can start this procedure, you must be logged in to the NM Client PC. Chromium must be installed on the PC, and the Compatibility View feature of Chromium must be disabled.

Procedure:

1. Open a web browser (Chromium) and enter the following URL address: `https://master-uis.ucs/ui`

   IMPORTANT:

   You must always log on to the Master UIS. The ability to back up and restore is provided by the Master UIS only. However, in case of a Master UIS switchover, the two following URLs should be used:

   - For MUIS01: `https://ucs-muis01.ucs/ui`
   - For MUIS02: `https://ucs-muis02.ucs/ui`
2. In the **User name** field, type a user name associated with the **Backup** user role.

3. In the **Password** field, type the password related to the user name.
4. Click **Log in**.

   You are logged in to the Upgrade Console and connected to the UIS in the zone that you specified in the first step of the procedure. The start page of the Upgrade Console appears showing a menu at the left and a welcome message.

2.9.1.2 AuC - Configuring a Backup

Prerequisites:
Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role.

Procedure:

1. Select **Backup Configuration** in the menu at the left side of the Upgrade Console.

   A table appears showing all applications that support backup in all zones residing in the cluster handled by the Upgrade Console.

2. If you want to save the backup file in the local storage of the zone UIS, select the check box of the **auc_active** application in the **Add To Backup/Restore** column. Make sure that you select the check box for the AuC application in the correct zone.

   NOTE: You can save the backup file in local as well as central storage. If the backup file is saved in both storages, the backup file from central storage is used, when you perform a data restoration.

3. If you want to save the backup file in the central storage of the Master UIS, select the check box of the **auc_active** application in the **Use Central Storage** column. Make sure that you select the check box for the AuC in the correct zone.

   NOTE: For redundant applications, the active application is indicated by the postfix **_active** in the name.

4. If you want to save the backup file in the Storage PC, select the check box of the **auc_active** application in the Use Storage PC column.

   NOTE: The backup file will be saved on all Storage PCs.

5. Click **Apply changes**.

   The **Backup** page appears showing applications selected for backup.

Postrequisites:
You now have these possibilities:

- If you want to create a backup file immediately, continue to AuC - Backing up Data On-Demand on page 55.
- If you want to create a scheduled backup task running at regular intervals, continue to AuC - Scheduling Backup on page 55.
- You can do both.

IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise the scheduled backup task for the application continues to run.

2.9.1.3 AuC - Backing up Data On-Demand

Prerequisites:
Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have configured the backup in advance.

Procedure:

1. Select **Backup** in the menu at the left side of the Upgrade Console.

   The **Backup** page appears showing applications selected for backup.

2. In the **Action** column of the **auc_active** application in the relevant zone, click **Run**.

   NOTE: For redundant applications, the active application is indicated by the postfix **_active** in the name.

   NOTE: You can also run a backup of several applications by selecting the check boxes of the applications in the check box column. Click **Run all selected** to initiate the backup.

   NOTE: When the backup task is initiated, the Enhanced Software Update tool finds out whether any of the redundant applications are active. If there is an active application, the backup is performed for this application. If none of the redundant applications are active, the backup fails.

   An indicator shows that the backup task is running. The **Backup Status** column shows the start and completion of the task. The backup file is created on the local storage of the application. Then it is transferred to the Zone UIS. If the **Use Central Storage** option was chosen, the file is transferred to the central storage. If the **Use Central Storage** and **Use Storage PC** options were chosen, the file is transferred to the Storage PC as well. If a backup file for the application exists, this backup file is deleted when the new file is saved. Only the most recent backup file is available. On a Storage PC, all backup files are kept.

Postrequisites: You now have these possibilities:

- If you want to create a scheduled backup task running at regular intervals, continue to AuC - Scheduling Backup on page 55.
- If you want to save the backup file on the NM Client PC, continue to AuC - Downloading a Backup File to the NM Client PC on page 56.
- If the backup file you just created satisfies your needs for backup, you do not have to do any further regarding backup.

2.9.1.4 AuC - Scheduling Backup

Prerequisites:
Before you can start this procedure, you must be logged in to the Upgrade Console on the Master UIS, with the **Backup** user role. You must have configured the backup in advance.

Procedure:

1. Select **Scheduled Backup** in the menu at the left side of the Upgrade Console.

   A table appears showing a list of scheduled backups. The date and time of the Master UIS is shown below the table.

2. Click **New**.

   A page appears allowing you to define the scheduled backup.

3. Do the following:
   a. In the **Name** field, type a name for the scheduled backup task.
   b. Click the browse button to select the zone, the subdomain, and the application for which the scheduled backup must be set up.

      A list appears in which you must click **Select** in the row containing the **auc_active** application in the relevant zone thereby selecting a zone, a subdomain, and an application at the same time.
   c. In the **Day** drop-down list, select a week day or select **DAILY**.
   d. In the **Hour** drop-down list, select at which hour the backup must run.
   e. In the **Minute** drop-down list, select at which minute the backup must run.
   f. Click **Submit**.

      NOTE: For redundant applications, the active application is indicated by the postfix **_active** in the name.

   You return to the **Scheduled Backup** page. The scheduled backup task that you created appears in the list of scheduled backups.

Postrequisites:
If your scheduled backup file has been created, and you want to save it on the NM Client PC, continue to AuC - Downloading a Backup File to the NM Client PC on page 56, otherwise you do not have to do any further regarding backup.

IMPORTANT: If you remove a backup for an application from the backup configuration, you also have to remove the scheduled backup task, if any, for this application. Otherwise the scheduled backup task for the application continues to run.

2.9.1.5
AuC - Downloading a Backup File to the NM Client PC

NOTE: If you do not need to save more than one backup file for the application, you can skip this procedure, and only save the backup file in the UIS backup storage.

Prerequisites:

IMPORTANT: If you use a Storage PC, this procedure is optional. Your backup is already saved to a Storage PC.

Before you can start this procedure, you must be logged in to the Upgrade Console with the **Backup** user role. A data backup file for the application must be available in the UIS backup storage. You want to download this backup file to the NM Client PC.

Procedure:

1. Select **Download Files** in the menu at the left side of the Upgrade Console.

   IMPORTANT: The backup file can be downloaded either from the Master UIS (which is a central backup storage) or from the Home UIS for the particular application.

   A table appears showing files available for download. If you are opening the **Download Files** page from an NM Client in a different zone, a warning appears.

2. Click **Download** for the relevant backup file.

   NOTE:
   The backup file is named `cluster`*<XX>*`_aucdb_01_`*<timestamp>*, where *<XX>* is the cluster ID, and *<timestamp>* is a date and time written as one row of digits with the format *<yyyymmddhhmm>*.

   You can only download one file at a time.

   A warning prompts you to decide whether you want to save the file.

3. Click **Save**.
4. In the **Save As** window, select a location for the file and click **Save**.